REMARKS

Claims 30-50 are pending. Applicant has cancelled claims 26-29 and amended claims 30, 38, and 46.

Applicant would like to thank the Examiner for her consideration during the telephone interview of June 28, 2006. During the interview, the Examiner and applicant's representative discussed the Section 103 rejection of the claims based on Wood and Lim. The Examiner indicated that Lim's "authentication profile" specifies an authentication methodology. The Examiner also requested that applicant point to sections of applicant's specification that support the language "after receiving the instruction" being added to the claims.

The Examiner has rejected claims 46-50 under 35 U.S.C. § 101 based on non-statutory subject matter. Although applicant disagrees, applicant has amended the claims to address the Examiner's concern. In particular, the claims now recite a "physical" computer-readable medium. (Specification, 9:6-22.)

The Examiner has rejected claims 30, 38, and 46 under 35 U.S.C. § 112, second paragraph, as being indefinite. Although applicant disagrees, applicant has amended the claims to address the Examiner's concern as to how a controlling client computer system is different from (i.e., separate from) a client computer system, and to further define authentication abilities and access rights.

With respect to claim 38, however, applicant does not understand what the Examiner means by "there is no explanation of how the server computing system has access to the authentication field and authentication methods." Applicant respectfully requests clarification.

With respect to claim 46, the Examiner believes it is unclear which computer system receives the instruction or authenticates the entity. Applicant respectfully disagrees. The preamble makes it clear that the instructions of the computer-readable medium control a

server computer system to receive and authenticate. With respect to claim 38, applicant respectfully submits that the preamble makes it clear that generating and sending are performed by the controlling client system.

The Examiner has rejected claims 30-50 under 35 U.S.C. § 103(a) as being unpatentable over Wood in view of Lim alone or in view of Lim in combination with what the Examiner believes is admitted prior art. Although applicant disagrees, applicant has amended the claims to more clearly claim the invention.

Lim describes a technique that provides a single login through which a user can access resources of multiple "protected servers." When a user initially logs in to Lim's Information Access System ("IAS"), the IAS relies on a remote security service (accessed via a proxy security server) to authenticate a user assuming self-registration. At initial login, the user provides a user id, password, and identification of a remote security service. (Lim, 9:59-10:5.) After the user is authenticated by the remote security service, the IAS stores the user id and password for the user. When the user subsequently logs in to the IAS, the IAS can authenticate the user using the user id and password rather than relying on the remote security service.

After the user is initially authenticated by a remote security service, the IAS requests the remote security service to provide authorizations indicating the resources that the user is authorized to access. The IAS stores those authorizations. When the user subsequently logs in to the IAS, the IAS can used the stored authorizations to control access to the resources without having the remote security service re-authenticate the user.

The Examiner points to column 5, line 61 through column 6, line 19 of Lim as describing "information on how a user should be authenticated." This section describes that during login a user is authenticated by the IAS based on the password in the Registry Server and the user may also be authenticated by a remote security server. So, this describes that the IAS "authenticates the user in one or more ways." (Lim, 6:5.)

Applicant's claims, in contrast, recite that "the authentication methodology being selected from multiple authentication methodologies [is] based on authentication abilities of the entity," or similar language. Lim does not select an authentication methodology. Rather, Lim simply authenticates a user based on the authentication methodology of the IAS and/or based on a remote security service. This is not selecting an authentication methodology. Rather, Lim always authenticates a user using the authentication methodology of the IAS if it can and always authenticates using a remote security service if a service is associated with the user and the IAS has not done so already. Lim thus does not select an authentication methodology from "multiple authentication abilities" as recited by the claims.

Lim's authentication profile does not include an indication of an authentication methodology selected from multiple authentication methodologies. Lim's authentication profile contains a user ID and password of a user along with a list of proxy security servers that can be used to authenticate the user. (Lim, 6:15-19.) Thus, Lim's authentication profile only identifies one authentication methodology that is one based on user ID and password. Lim's authentication profile thus does not suggest or imply multiple authentication methodologies.

Moreover, applicant has amended the claims to further distinguish Lim. In particular, the claims now make it clear that the "instruction that indicates the authentication methodology" is received before the user requests to login. For example, claim 46 recites that a server computer system, "after receiving the instruction from the controlling entity, receiv[es] a request from the entity to access a service of the server computer system." The Examiner believes that Lim's Registry Server corresponds to the "controlling entity" of the claims, that Lim's Authentication and Authorization module corresponds to the "server computer system" of the claims, and that Lim's "authentication profile" corresponds to the "instruction" of the claims. Lim's Authentication and Authorization module, however, retrieves the authentication profile of the user from the

Registry Server after the user requests to login. Thus, the combination of Wood and Lim do not describe this further distinguishing feature of the claims.

During the telephone interview, the Examiner requested that applicant point to portions of the specification that support the language "after receiving the instruction, receiving a request from the client computer system to access a service." Support for this language is provided in the specification at 6:12-20 and 22:22-23:10. In particular, the specification states that:

> The request [that includes an instruction] is then transmitted to the server computer system. When receiving subsequent requests for service . . ., the server computer system will refer to information in the instruction.

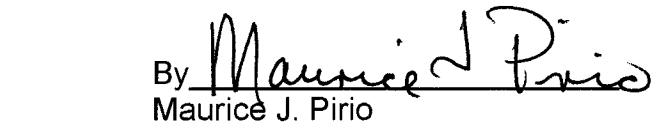
(Specification, 6:16-19, emphasis added.)

The term "subsequent" refers to the receiving of the transmitted request that includes the instruction "identifying an authentication method." Thus, the "after receiving the instruction" language of the claims is fully supported by the specification.

Based upon these remarks, applicant respectfully requests reconsideration of this application and its early allowance. If the Examiner has any questions or believes a telephone conference would expedite prosecution of this application, the Examiner is encouraged to call the undersigned at (206) 359-8548.

Dated: July 14, 2006

Respectfully submitted,

By 

Maurice J. Pirio
Registration No.: 33,273
PERKINS COIE LLP
P.O. Box 1247
Seattle, Washington 98111-1247
(206) 359-8548
(206) 359-9548 (Fax)
Attorney for Applicant